XXI CONGRESO INTERNACIONAL
SOCIEDAD ESPAÑOLA DE PERIODÍSTICA

Repensar los valores clásicos del periodismo. El desafío de una profesión enred@da

Actas de las comunicaciones presentadas en el congreso

Jorge Miguel Rodríguez Rodríguez (ed.)

Sociedad Española de Periodística SEP

Universidad San Jorge

Edita: Sociedad Española de Periodística
Universidad San Jorge

Fecha de edición: diciembre 2015

ISBN: 978-84-608-3103-7

Depósito Legal: Z 1729-2015

LA CIBERGUERRA COMO NUEVA ESTRATEGIA BÉLICA EN EL CONTEXTO INTERNACIONAL Y SU TRATAMIENTO PERIODÍSTICO EN ESPAÑA

Noelia García Estévez
Universidad de Sevilla
noeliagarcia@us.es

Resumen: El avance de las tecnologías y el desarrollo digital ha transmutado aspectos fundamentales en el devenir social. Tal es así que incluso ha incidido en las tácticas de presión, ofensivas y ataques de un país contra otro, de un grupo armado en contra del gobierno, o ataques individuales de uno o varios hackers.

Esta investigación pretende examinar el origen, desarrollo y situación actual de estos conflictos de carácter tecnológico a la vez que profundizar en las diversas técnicas de ataque empleadas por sus contendientes. De igual forma, es objetivo de esta comunicación realizar un análisis de contenido del tratamiento informativo otorgado por los medios españoles a este fenómeno de alcance mundial.

Palabras clave: ciberguerra, guerra digital, guerra informática, hacktivismo, periodismo.

1. INTRODUCCIÓN

Partimos de una realidad social cambiante, compleja y diversa donde el entorno web se integra radicalmente en la misma y sin el cual sería imposible describir y entender el actual tejido social. Vivimos en una era tecnológica donde tiene lugar una revolución digital capaz de modificar conceptos y actitudes. De hecho, nuestra sociedad ha experimentado un importante giro en el propio desarrollo de la ciudadanía, sus hábitos, costumbres y maneras de proceder. La inclusión de una esfera digital predominante y el imparable desarrollo tecnológico han propiciado un nuevo contexto en el que es preciso reformular las significaciones tradicionales, los imaginarios sociales y las actividades cívicas. Recordemos la tesis de Echeverría según la cual existen tres entornos de la humanidad: el entorno primero o Physis, el entorno segundo o Polis y el entorno tercero o Telépolis. El primer entorno se refiere a todo aquello que es natural, el segundo trata del espacio social y cultural y el tercero hace referencia a un escenario "que difiere profundamente de los entornos naturales y urbanos en los que tradicionalmente han vivido y actuado los seres

humanos" (Echeverría, 1999, p. 14). Se refiere a un entorno articulado a través de las Tecnologías de la Información y la Comunicación y en el que se han visto sustancialmente modificadas las relaciones sociales y culturales que se dan y daban en los entornos primero y segundo.

2. METODOLOGÍA

El desarrollo tecnológico y la penetración digital en la sociedad actual es una evidencia palpable a estas alturas. Ello ha transmutado no solo nuestras formas de comunicarnos y de sociabilizar, nuestras rutinas de trabajo o nuestros hábitos de consumo y de ocio sino que también ha incidido en las tácticas de presión, ofensivas y ataques de un país contra otro, de un grupo armado en contra del gobierno, o ataques individuales de uno o varios hackers.

Asistimos pues a una nueva estrategia bélica cuyo escenario se ha trasladado al ciberespacio y donde las Tecnologías de la Información y la Comunicación se han convertido en las poderosas armas para derrotar al enemigo. Una vez superada la Guerra Fría, vivimos ahora una nueva guerra en la que es más factible vencer al adversario atacando su infraestructura informática que empleando cualquier otro tipo de ataque físico.

Esta investigación pretende examinar el origen, desarrollo y situación actual de estos conflictos de carácter tecnológico a la vez que profundizar en las diversas técnicas de ataque empleadas por sus contendientes. De igual forma, es objetivo de esta comunicación realizar un análisis de contenido del tratamiento informativo otorgado por los medios españoles a este fenómeno de alcance mundial. Para ello hemos seleccionado las ediciones impresas de los periódicos *ABC*, *El Mundo* y *El País* siendo nuestro objeto de estudio todos los contenidos relativos a esta temática publicados a lo largo del 2014.

Dada la naturaleza compleja de nuestra temática hemos optado por la utilización de una combinación metodológica cualitativa y cuantitativa a través del desarrollo de un método empírico analítico considerando pautas sistemáticas, sintéticas, deductivas e inductivas. En nuestra investigación toman sentido especialmente el método empírico-analítico, pues nos permiten descomponer el problema propuesto como objeto de estudio en sus aspectos más básicos y fundamentales, lo cual nos posibilita aplicar métodos experimentales. En cuanto a la estructura del proceso investigador, hemos tenido en cuenta el método hipotético-deductivo, pues partimos de la observación para posteriormente plantear las hipótesis que habrán de ser verificadas. No olvidemos que abordamos el estudio de un fenómeno

coetáneo, extraordinariamente cambiante y de difícil delimitación, por lo que nos hemos decantado por una postura abierta conscientes de que nuestro objeto de estudio está en continua relación con la dinámica de cambio en tiempo y espacio.

3. EL HACKTIVISMO MÁS ALLÁ DEL MILITAR

El influjo y la penetración de las tecnologías en la sociedad a través de una apropiación tecnológica y digital se desarrolla en el orbe cibernético hallando en él una herramienta tecno-cívica. Confían en el valor social y político de la tecnología fomentando un *hackerismo* que va mucho más allá del placer de experimentar con las TIC y aprender de ello. Entienden que la tecnología se ha convertido en mediadores necesarios para la emergencia de nuevas formas de sociabilidad (Aceros, 2006). El mundo del software tiene implicaciones sociales, con el compromiso ciudadano de acercar "herramientas de interacción tecno-políticas a la gente corriente" (Garaizar, 2004: 10). Los miembros de este movimiento parten de una conciencia colectiva y adquieren una actitud comprometida socialmente poniendo sus conocimientos al servicio de la ciudadanía y promoviendo políticas tales como la libertad de expresión, los derechos humanos y la ética de la información.

El término *hacktivismo* fue usado por primera vez en un artículo de la artista multimedia Shu Lea Cheang publicado en *InfoNation* en 1995; un año después sería utilizado por un miembro del grupo de *hackers* americano Cult of the Dead Cow (cDc). Pero será en el año 2000 cuando Oxford Ruffin, otro miembro del citado grupo, escriba que "los hacktivistas emplean tecnología para defender los derechos humanos" (Paget, 2012: 3).

Podemos definir el *hacktivismo* como "la utilización no-violenta de herramientas digitales ilegales o legalmente ambiguas persiguiendo fines políticos. Estas herramientas incluyen desfiguraciones de webs, redirecciones, ataques de denegación de servicio, robo de información, parodias de sitios web, sustituciones virtuales, sabotajes virtuales y desarrollo de software" (Alexandra citado en Wikipedia, 2014). El *hacktivismo* combina pues elementos del *hacking online* y del activismo político (Denning, 2003). Lejos del estereotipo de personas introvertidas, aisladas y exclusivamente obsesionadas con la programación y la seguridad informática, muchos *hackers* toman consciencia de las dimensiones políticas del código que escriben y se lanzan para amplificar sus efectos políticos.

El uso político que hacen los *hacktivistas* los diferencian de los *hackers* ya que, normalmente, este último es "un personaje apolítico que sólo lucha por sus compañeros, por la libertad

de la información y por sí mismo" (Vicente, 2004). En cambio, para los *hacktivistas* los puntos de partida coinciden con los principios consagrados en la Declaración Universal de Derechos Humanos y la Convención Internacional sobre Derechos Civiles y Políticos. Tampoco podemos vincular estos movimientos *hacktivistas* con los *crackers*, "cuyo objetivo es el de crear virus e introducirse en otros sistemas para robar información y luego venderla al mejor postor" (Vicente, 2004). De igual forma, surgen en el seno del *hacktivismo* una escisión que se aleja del compromiso cívico y de la que resultan los conocidos como *script kiddies*, jóvenes que intentan hacerse pasar por *hacker*, a pesar de su falta de habilidades técnicas ni experiencia en sistemas informáticos, y con ganas de "piratear por piratear" (Paget, 2012: 9).

Las incipientes actuaciones *hacktivistas* estuvieron protagonizadas por grupos como Electronic Disturbance Theatre; Electrohippies; Cult of the Dead Cow; Hactivist.com; Critical Art Ensemble; o HispanoTecno.Net. Desde mediados de los años noventa se han llevado a cabo una serie de acciones concretas *hacktivistas* con un predominio de *hacklabs* y *hackmeetings*, instancias de diálogo de *hackers* que lo consolidan como un movimiento social articulado dentro y fuera de la red. Desde el punto de vista de estructuras sociales, estos movimientos canalizan su acción en tres dimensiones: la solidaridad, es decir, el mutuo reconocimiento de los actores como miembros de una misma unidad social; el conflicto con un adversario por la apropiación y control de recursos valorados por ambos; y la ruptura de los límites de compatibilidad del sistema en el que acontece la movilización (Melucci, 1999).

Las técnicas empleadas hoy día por los grupos *hacktivistas* son diversas y variadas, en función de los objetivos, de los agentes implicados, de la naturaleza de la reivindicación, etc. En general, podemos establecer una tipología básica que suelen regir las características y dinámicas de acción de estos colectivos:

- Un ataque DDoS (*distributed denial of service attack* o ataque distribuido de denegación de servicio) es una técnica *hacker*, bastante antigua en el mundo del ciberespacio, consistente en un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible para los usuarios legítimos. Se genera mediante la saturación de los puertos con flujo de información, haciendo que el servidor se sobrecargue y no pueda seguir prestando servicios, por eso se le denomina "denegación", pues hace que el servidor no dé abasto a la cantidad de solicitudes. La forma más habitual de este tipo de ataques se realizan a través de programas

informáticos bastantes sencillos (como LOIC) que permiten entrar gran cantidad de veces a un sitio web en concreto de forma automatizada y con una identidad falsa (*botnets*), de tal forma que, al realizar tal volumen de peticiones de datos a un servidor y desde tantos puntos al mismo tiempo, estos intentos de conexión consumen recursos en el servidor y limitan el número de conexiones que se pueden hacer, reduciendo la disponibilidad del servidor para responder otras peticiones legítimas de conexión.

- Los ataques *netstrike* consisten en la interacción consensuada de multitud de personas desde diferentes lugares y distintos horarios sobre un sitio web, con objetivo de ralentizar su servicio, llegando en ocasiones a saturar la web. En este caso los atacantes son personas conscientes de su acción, al contrario que en el caso anterior donde se emplean en su mayoría zombies (ordenadores que atacan automáticamente a través de algún virus o troyano)
- Se utilizan *exploits*, fragmentos de software o secuencias de comandos y/o acciones, con el fin de aprovechar una vulnerabilidad de seguridad de un sistema de información para conseguir un comportamiento no deseado del mismo.
- El *doxing* consiste en publicar fotos, información de contactos y datos personales y familiares en represalia por una acción llevada a cabo por un individuo o grupo de individuos.
- El *copwatching* es publicar en sitios web especiales información identificativa y observaciones relacionadas con los miembros de las fuerzas de seguridad.
- El *google bomb* es un método mediante el cual es posible colocar ciertos sitios web en los primeros lugares de los resultados de una búsqueda en Google utilizando un texto determinado.
- Los *fakes* son falsificaciones o engaños que pretende suplantar una institución o campaña oficial el mayor tiempo posible.
- Redirección de las páginas web institucionales u oficiales.
- Desarrollo de herramientas de software (*rootkits*, *keyloggers*, etc.).
- Robo de datos y filtraciones, a través de ataques de inyección SQL, por ejemplo.
- Etc.

4. EL CIBERCONTROL Y LA CIBERSEGURIDAD

Internet se presenta como una red global con poder de procesamiento de la información y comunicación multinodal, no distinguiendo fronteras y estableciendo una comunicación

irrestricta entre todos sus nodos (Castells, 2001, parra 3). Resurge con más fuerza un derecho universal que alcanza, o debería alcanzar, su mayor garantía en el ciberespacio: la libertad de expresión. Bustamante (2001) habla de una cuarta generación de derechos humanos surgida a partir de la inclusión social de las TIC donde "la universalización del acceso a la tecnología, la libertad de expresión en la Red y la libre distribución de la información juegan un papel fundamental" (parra 10). Ya en la Declaración Universal de los Derechos Humanos de 1948 aparece reconocido el derecho a la libertad de pensamiento, de conciencia y de religión (art. 18), la libertad de investigar y de recibir información (art. 19), y la libertad de opinión y de difundirla sin limitación de fronteras, por cualquier medio de expresión (art. 19). Sin estas libertades se hace imposible la instauración de una sociedad civil activa y participativa dentro de la dinámica de las democracias.

Ahora bien, como afirma Castells (2001, parra 4) "si la red es global, el acceso es local, a través de un servidor. Y es en este punto de contacto entre cada ordenador y la red global en donde se produce el control más directo". Es decir, si "técnicamente, Internet es una arquitectura de libertad. Socialmente, sus usuarios pueden ser reprimidos y vigilados" (parra 7). En efecto, no son pocas las medidas y estrategias llevadas a cabo por los diferentes gobiernos y grupos de poder para controlar y vigilar los espacios en línea.

La empresa en consultoría y tecnología Indra[1] entiende que las soluciones sectoriales en el ámbito de la ciberseguridad atañen a tres ámbitos:

- Ciberseguridad para el ciudadano, que engloba la protección integral del ciudadano como usuario de internet que realiza diversidad de gestiones.
- Ciberseguridad para las organizaciones, ya sean públicas y privadas.
- Ciberseguridad en Infraestructuras críticas, entendiendo por críticas aquellas cuyas consecuencias de una posible vulneración afecta de manera transversal al resto de sectores sociales.

Es misión de un Estado garantizar la seguridad en los tres apartados anteriores para garantizar el buen funcionamiento de sus instituciones y un desarrollo normal del conjunto de la ciudadanía. Sin embargo, diversos autores como Cáceres (2004) consideran que los distintos gobiernos de diversas ideologías y regímenes políticos se han valido del pretexto

[1] Indra es una multinacional de Consultoría y Tecnología líder en España y Latinoamérica. Ofrece soluciones y servicios tecnológicos para los sectores de Transporte y Tráfico, Energía e Industria, Administración Pública y Sanidad, Servicios Financieros, Seguridad y Defensa y Telecom y Media. Véase más en www.indracompany.com.

de defender la seguridad nacional o preservar la unidad o valores nacionales para impedir a sus ciudadanos un acceso libre a Internet. Así lo corrobora el informe "Enemigos de Internet" elaborado por Reporteros Sin Fronteras (2014), en el que revela que organismos gubernamentales y agencias implementan la censura y la vigilancia online. Los casos más extremos los hallamos en organismos como la Autoridad de Telecomunicaciones de Pakistán, el Centro Científico y la Agencia de Información Tecnológica de Corea del Norte, el Ministerio de Información y Comunicaciones de Vietnam o la Oficina Estatal de Información de Internet de China que han usado la defensa de la seguridad como pivote para ir mucho más allá de su misión original con el fin de censurar a periodistas, blogueros y otros proveedores de información.

Pero tales actuaciones también las encontramos, según este informe, en democracias que tradicionalmente se han jactado de defender la libertad de expresión y el libre flujo de información. Así, podemos citar a la NSA (Agencia de Seguridad Nacional) en Estados Unidos, el GCHQ (Cuartel General de Comunicaciones del Gobierno) en el Reino Unido o el Centro de Desarrollo Telemático de la India. También es polémica la herramienta SITEL (Sistema Integrado de Interceptación de Telecomunicaciones) puesta en marcha en 2001 en España y que permite al Gobierno interceptar y grabar en tiempo real cualquier conversación telefónica, correo electrónico o mensaje de móvil, además de almacenar en formato digital todos los datos de esas comunicaciones para su posterior análisis. El programa lo controla el Ministerio del Interior, lo utilizan indistintamente la Guardia Civil, el Cuerpo Nacional de Policía y el Centro Nacional de Inteligencia y su aplicación requiere de la imprescindible colaboración de las operadoras privadas (Lobo, 2013).

En todo este entramado se precisa de la ayuda de las empresas del sector privado que funcionan como facilitadoras de información y datos a los organismos solicitantes incluso antes de haber una orden judicial. Reporteros Sin Fronteras (2014) critica duramente a "las compañías que ponen sus conocimientos al servicio de los regímenes autoritarios a cambio de sumas de dinero a menudo colosales". Del mismo modo, Pete Ashdown, fundador de XMission, denunció que "gigantes como Google, Microsoft o Apple seguramente se benefician económicamente al permitir que la NSA obtenga datos de sus redes" (Ashdown citado en RT, 2013).

Las redes sociales también se han convertido en puntos de interés estratégicos para los gobiernos y agencias que no dudan en establecer solicitudes de información sobre sus internautas a las mismas. En este sentido, y en un intento de ofrecer transparencia y

confianza a sus usuarios, el gigante Facebook publica periódicamente informes sobre las solicitudes de los gobiernos y en los que se detallan los siguientes datos: países que solicitaron a Facebook información sobre los usuarios; número de solicitudes recibidas de cada uno de esos países; número de usuarios/cuentas de usuario especificados en esas solicitudes; y porcentaje de solicitudes en las que Facebook estaba obligado por ley a revelar al menos algunos datos (Facebook, 2013). Hasta la fecha ha publicado dos informes, correspondientes al primer y segundo semestre de 2013, y en ambos Estados Unidos es el país que más peticiones ha tramitado siendo en torno a 24.000 a lo largo del pasado año y de las cuales fueron atendidas un 80% aproximadamente (Facebook, 2014).

En la 'sobremodernidad' en la que vivimos el cibercontrol se ayuda de una cibervigilancia conformando una sociedad vigilada que ha venido a derivar en lo que Deliuza denominó la "sociedad del control". Por primera vez en la historia las técnicas y estrategias utilizadas se basan en la invisibilidad y ubicuidad de los dispositivos que nos vigilan pero, a pesar de ello, el individuo se halla encerrado en un espacio en el que se siente vigilado.

> Los enfrentamientos violentos y directos han sido eliminados trasladando el campo de batalla al foro interno de la persona. El condicionamiento exigido por las normas sociales toma el carácter de una autocoerción y da lugar a la formación de un superó individual que invita a que cada individuo adopte el comportamiento que de él se espera (Mattelart y Vitalis, 2015, p. 190).

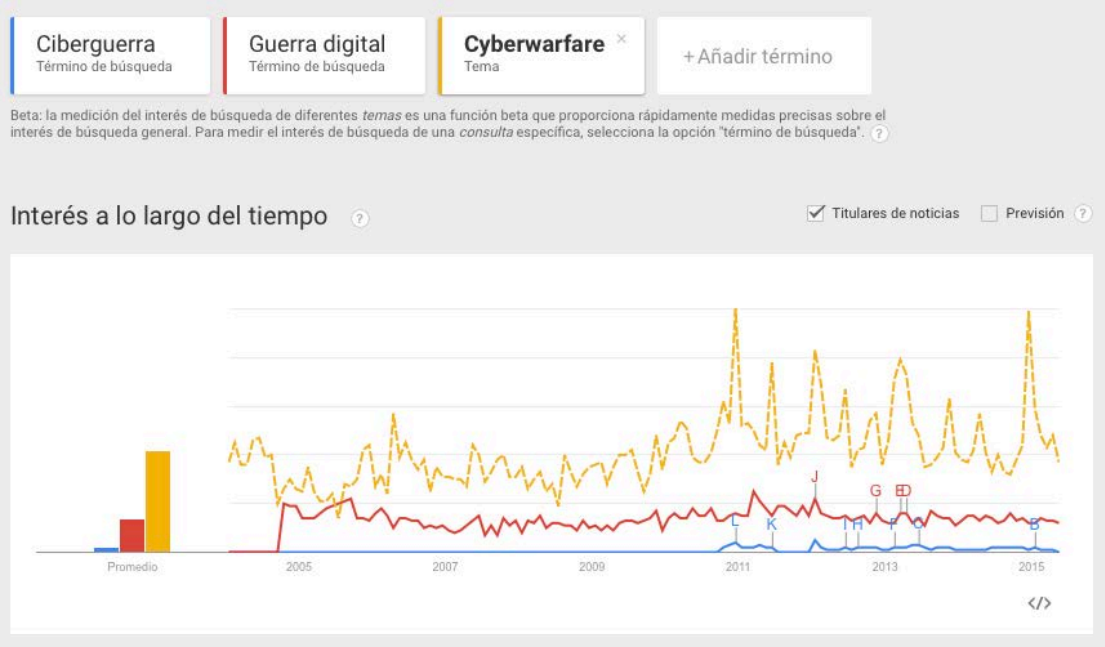
5. HACIA UNA DEFINICIÓN DE CIBERGUERRA

Alcanzar una definición concreta y consensuada del concepto ciberguerra es una tarea bastante compleja. Partimos de la idea básica que en la ciberguerra se realizan ataques digitales a sistemas y estructuras informáticas. En este apartado del trabajo pretendemos hacer un breve repaso por algunas de las definiciones ofrecidas por diversos autores con el fin de clarificar un poco este concepto.

En primer lugar hemos de hacer referencia al estado poco maduro de este concepto que apenas si lleva empleándose de manera habitual desde hace cinco años. En la siguiente imagen podemos comprobar cómo ha sido la evolución de búsquedas en Internet de tres acepciones relacionadas con nuestro objetivo de estudio. La palabra en inglés 'cyberwafare' es la más longeva y la que muestra mayor interés desde el principio, haciendo su irrupción hace más de una década y aumentando su atención a lo largo del tiempo. En segundo, nos encontramos con el concepto de 'guerra digital' que, sin tener índices tan altos como el

caso anterior, también se ha mantenido vigente en un prolongado periodo de tiempo. Ahora bien, llegamos al término 'ciberguerra' y descubrimos que es a partir de 2011 cuando empieza a tener fuerza y, si bien su evolución va en aumento, aún dista mucho de la proliferación de los dos conceptos anteriormente mencionados.

Imagen 1. Interés de búsqueda en Internet de los conceptos 'ciberguerra', 'guerra digital' y 'cyberwafare'.



Fuente: Google Trends, mayo de 2015

Del mismo modo que el entorno online se ha convertido en parte importante de las acciones cívicas y sociales o de grupos de hacker que lo utilizan como instrumento de presión social y política, los gobiernos y estados han puesto la mira en estos contextos como nuevos espacios de batalla en los que pueden atacar y deben defenderse:

> Cada vez hay más evidencias de que los Estados avanzados invierten recursos en desarrollar y comprar virus informáticos, programas espías ('spyware'), vulnerabilidades en sistemas y 'software' intrusivo como una estrategia para reforzar la 'ciberseguridad', la capacidad de respuesta a un 'ciberataque' y lo que parece más importante, la capacidad de 'ciberatacar' primero. (Romero, 2015).

Estamos de acuerdo con Wegener en que en general los ataques digitales, incluyendo aquellos con objetivos militares, son, "primordialmente, no violentos y de un coste relativamente bajo (bits en lugar de bombas»), y se desarrollan exclusivamente a través de la invasión electrónica de sistemas y estructuras de red" (2013, p. 181). Sin embargo hemos de

precisar que el hecho de que se definan como no violentos no significa que de sus acciones no haya víctimas resultantes, tanto militares como civiles. Así lo afirman Clarke y Knake cuando sostienen que la ciberguerra no es simplemente una nueva forma de confrontación bélica desprovista de víctimas o limpia, ni algún tipo de arma secreta que sea necesario mantener oculta a la opinión pública, "pues es la población civil y las corporaciones de titularidad pública que dirigen nuestros sistemas clave los que con más probabilidad sufran las consecuencias de una 'ciberguerra'" (2011). Esto es, las consecuencias de estos ataques informáticos con fines militares y beligerantes tienen unas fuertes, aunque silenciosas, repercusiones en el conjunto de la sociedad civil afectada.

Además, hemos de ser conscientes de que cuando nos referimos a ciberguerra no solamente estamos hablando de un conflicto u ataque entre gobiernos, sino que también entran en juego otras organizaciones, como grupos terroristas, empresas u organizaciones criminales transnacionales. Y es que son muchos los intereses que pueden llevar a la culminación de un ataque informático: objetivos militares de naciones y estados, fines terroristas (ciberterrorismo), protestas civiles y ciudadanas, propósitos financieros como la piratería industrial o con un carácter científico-investigador tratando de aumentar la sensibilidad de este tema mediante la investigación y la publicación de las nuevas amenazas de seguridad. En este sentido es importante establecer una frontera entre un ataque cibernético puntual y un ataque de ciberguerra en un contexto global. Para Ferrero (2013) el límite entre uno y otro radica en la importancia y consecuencias de este ataque reflejado en la interrupción que produce en la vida nacional o en cualquiera de sus instituciones críticas.

A estas alturas se entiende que el ciberespacio es el quinto escenario bélico, junto con el terrestre, el marítimo, el aéreo y el espacial. En los Estados Unidos el Pentágono ha reconocido formalmente el ciberespacio como un nuevo dominio de guerra como donde desarrollar operaciones militares como las de tierra, mar, aire y espacio (Lynn, 2010). Atendiendo a la autoría los ciberataques se pueden clasificar en (Ferrero, 2013):

1. Patrocinados por Estados. En estos últimos años se han detectado contra las infraestructuras o contra objetivos concretos. Entre los más conocidos están el ataque a Estonia en el 2007, que supuso la inutilización temporal de muchas de sus infraestructuras críticas; los sufridos por las redes clasificadas estadounidenses, producidos por atacantes basados en China; el último ataque por virus a los

sistemas informáticos de decenas de industrias iraníes, reconocido por Irán y del que dice haberse recuperado. Aquí puede también incluirse el espionaje industrial.

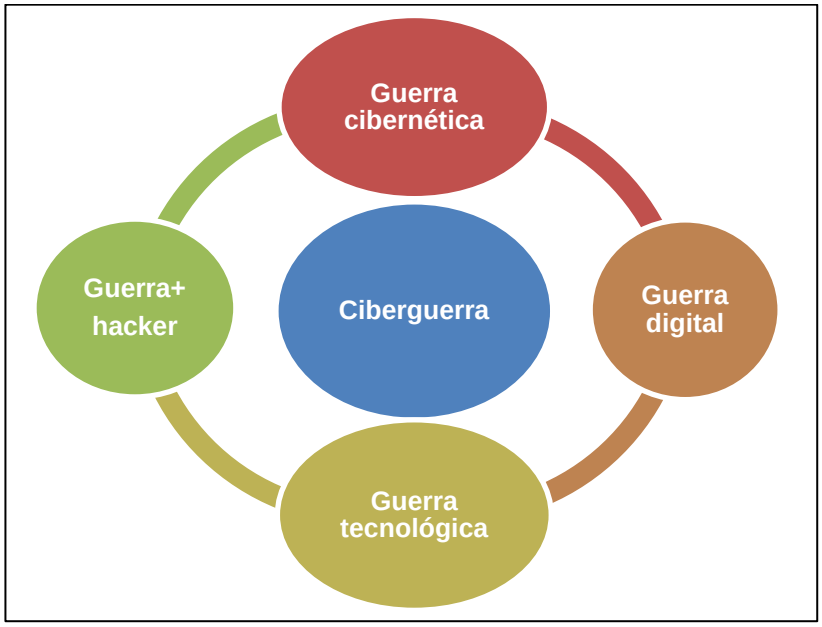
2. Servicios de inteligencia y contrainteligencia. Los Estados suelen disponer de bastantes medios tecnológicos avanzados.
3. Terrorismo y extremismo político e ideológico. Utilizan el ciberespacio para planificar sus acciones publicitarias y como herramienta de financiación.
4. Ataques de delincuencia organizada. Su objetivo es la obtención de información para conseguir beneficios económicos.
5. Ataques de perfil bajo. Ataques de naturaleza muy heterogénea ejecutados por personas con conocimientos TIC.

En los últimos años se han producido eventos que han provocado grandes giros estratégicos en el planeamiento de la defensa nacional. Desde el punto de vista del posicionamiento táctico de un país ha adquirido mayor envergadura el equipamiento ante las amenazas tipificadas como irregulares y/o híbridas, la guerra asimétrica, el conflicto de baja intensidad o los ataques informáticos. De hecho, actualmente encontramos países como China, Irán, Rusia, Corea del Norte o Pakistán que han reconocido abiertamente su interés en reforzar unas tácticas estratégicas en el ciberespacio como instrumento con el que lograr un liderazgo político y económico en sus áreas geográficas de influencia. Así lo corroboran las inversiones económicas destinadas a recursos tecnológicos y la formación del capital humano con el objetivo de preparar una defensa fuerte y una beligerancia activa en el ciberespacio.

6. ESTUDIO DE CASOS Y DISCUSIÓN DE LOS RESULTADOS

Como ya avanzamos en el apartado de metodología, para investigar nuestro objeto de estudio y su tratamiento periodístico en España hemos seleccionado tres unidades de muestra de referencia como son las cabeceras impresas de *ABC*, *El Mundo* y *El País* y una horquilla temporal de un año, desde el 1 de enero hasta el 31 de diciembre de 2014. A la hora de buscar y seleccionar los textos periodísticos que han sido objeto de estudio nos hemos planteado una serie de palabras clave que nos han permitido tal indagación (véase Imagen 2). Tras la búsqueda y selección nos han resultado un total de 34 textos periodísticos en el conjunto de los tres medios analizados.

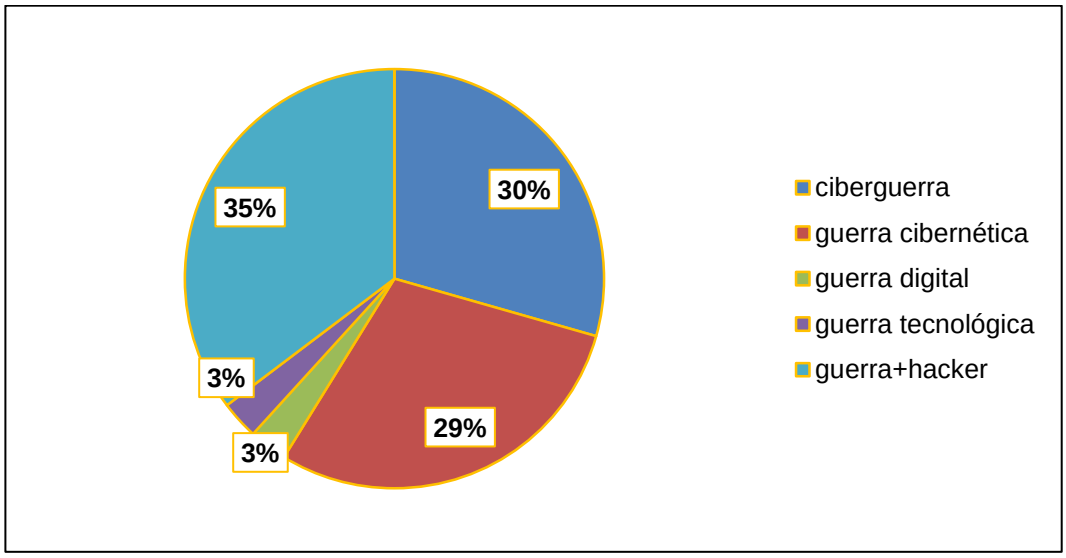
Imagen 2. Palabras clave empleadas para la selección de textos periodísticos



Fuente: elaboración propia

Cabe destacar a este respecto que, a pesar del interés suscitado en torno a este concepto en los último años (recuérdese la Imagen 1 sobre la cantidad de búsquedas realizadas en Google) y de que cada vez más los políticos y gobernantes empiecen a usar esta terminología, encontramos aún pocas referencia explícitas en la prensa española. Solo 34 piezas informativas incluían como tema central o secundario la temática de la guerra tecnológica. En relación con las palabras clave que se imponían en cada uno de esos 34 textos periodísticos, la mayor predominancia ha resultado de la combinación de las palabras 'guerra+hacker', que supone un 35% del total. El segundo término más empleado por los periodistas españoles es precisamente el de 'ciberguerra', con un 30%. Le sigue muy de cerca los conceptos unidos de 'guerra cibernética', que han sido utilizados en un 29% de los casos encontrados. Menos frecuente es el uso de 'guerra digital' o 'guerra tecnológica' que solo han sido esgrimidos en un 3% de los textos, respectivamente.

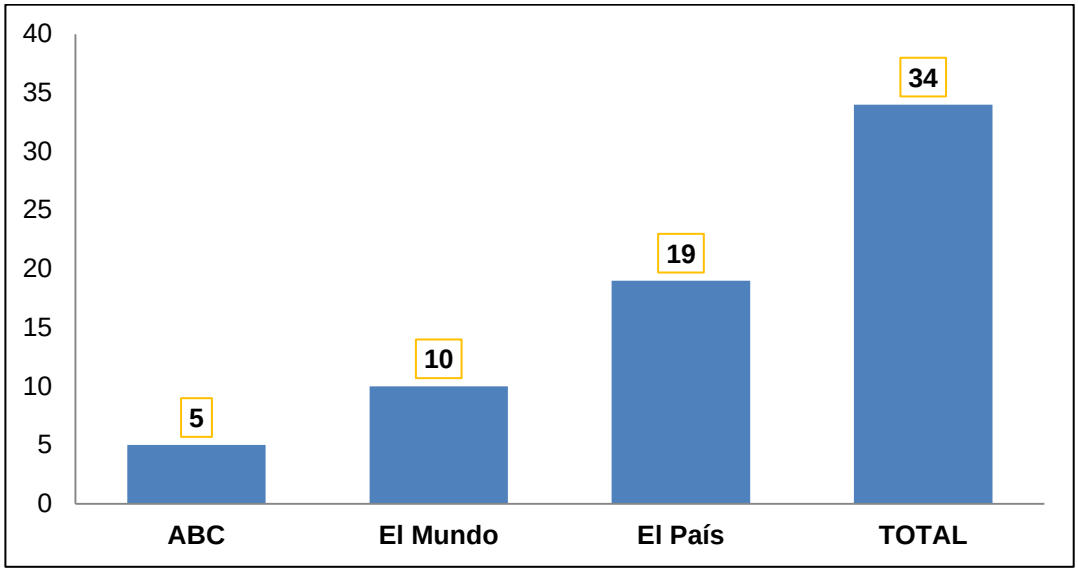
Gráfico 1. Porcentaje de uso de los conceptos relacionados con la ciberguerra en los textos periodísticos



Fuente: elaboración propia

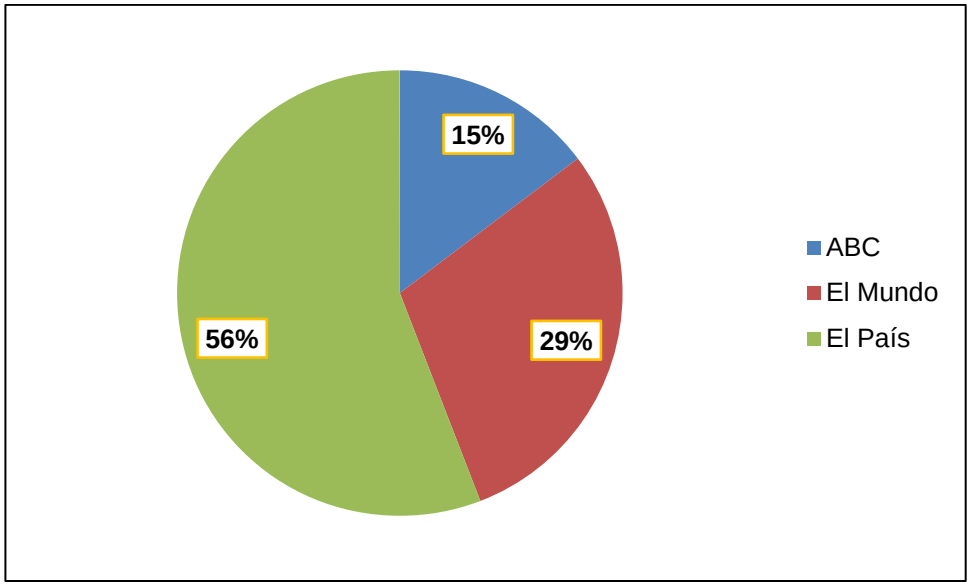
En un análisis pormenorizado de cada medio de comunicación observamos también notables diferencias en el tratamiento otorgado por cada una de las cabeceras. Si, como hemos dicho, en el conjunto hemos hallado un total de 34 textos, esta cifra se reduce hasta 5 en el caso del diario *ABC*, que es el que menor espacio le dedica a este tipo de asuntos. Por su parte, es el periódico *El País* el que mayor importancia le adjudica a esta temática incluyendo hasta 19 informaciones relativas a ello a lo largo de 2014. El diario *El Mundo* se encuentra en un escalafón intermedio, habiendo incluido 10 informaciones sobre la ciberguerra y los ataques tecnológicos.

Gráfico 2. Cantidad de noticias sobre ciberguerra en la prensa española



Fuente: elaboración propia

Gráfico 3. Porcentaje de textos informativos sobre ciberguerra en la prensa española

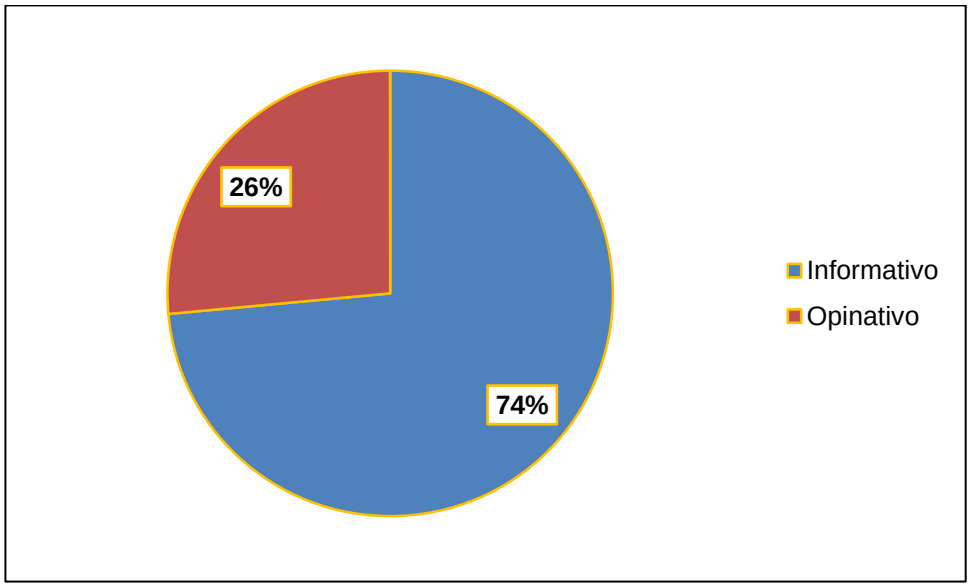


Fuente: elaboración propia

También es revelador del tipo de cobertura informativa conocer los géneros empleados. En concreto, para determinar la importancia dada a un tema es significativo detectar si a las piezas meramente informativas, las más habituales en los periódicos, se han añadido otros géneros que permiten detenerse más en el asunto en cuestión. Así, la inclusión de artículos de opinión revela que el periódico ha destacado dicho acontecimiento respecto al resto de los sucesos acontecidos. Como cabía esperar, la mayoría de las unidades analizadas son

noticias o reportajes informativos. En líneas generales, la mayora cantidad de textos periodísticos relativas a la temática de la ciberguerra y los ataques informáticos con fines militares y políticos se corresponde con los géneros informativos, representando un 74% con respecto al total. Es decir, en el conjunto de los tres medios analizados, solo 1 de cada cuatro piezas informativas era tratada desde un punto de vista opinativo y valorativo.

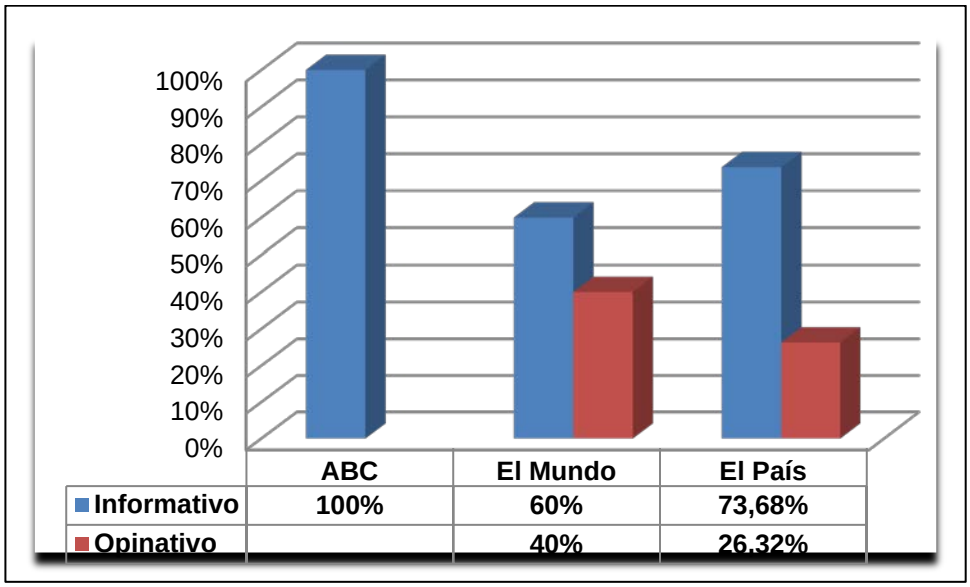
Gráfico 4. Porcentaje del género empleado en los textos periodístico sobre ciberguerra



Fuente: elaboración propia

Las diferencias vuelven a ser más acusadas cuando realizamos un análisis concreto e independiente de cada una de las cabeceras. Como se observa en el siguiente gráfico, es el periódico *El Mundo* el que considera que la guerra cibernética como asunto de actualidad debe ser tratado con más ahínco desde una perspectiva reflexiva y de opinión, ayudando a sus lectores a conformar una idea cercana al fenómeno y a posicionarse ante él. De este modo, un 60% de sus textos son informativos mientras que el 40 restante pertenecen al género de la opinión. *El País*, por su parte, también incluye con relativa frecuencia textos opinativos que complementen las informaciones estrictas concernientes a la temática que aquí nos ocupa, siendo un 26,32% de carácter reflexivo. Es el diario *ABC* en el que no hemos hallado en todo el año de estudio ningún texto que no fuera informativo y que abarcara asuntos relativos a las estrategias de guerra basadas en Internet y en las Tecnologías.

Gráfico 5. Porcentaje del género empleado en los textos periodístico sobre ciberguerra según el medio de comunicación



Fuente: elaboración propia

7. CONCLUSIONES

Esta investigación desarrolla un recorrido analítico descriptivo de la situación actual de los actuales aplicaciones de herramientas tecnológicas con fines bélicos, así como la instauración del ciberespacio como el quinto escenario bélico. El desarrollo tecnológico junto con el avance de Internet ha marcado un punto de inflexión en el propio devenir ciudadano y las propias dinámicas de actuación sociales y ciudadanas y políticas y gubernamentales.

En entorno online es entendido como un espacio de desarrollo democrático e igualitario donde la libertad de expresión y de circulación de ideas debe tener su máxima expresión. Sin embargo, los gobiernos e instrumentos de poder cada vez más están instaurando mecanismos de control y vigilancia basados en el pretexto de una ciberseguridad nacional y ciudadanas. Ello genera un nuevo contexto en el que el hackerismo retoma más fuera y pone a prueba estas medidas coercitivas.

En el contexto internacional actual imperan nuevas fórmulas de control y de dominación, mucho más sutiles que los convencionales enfrentamientos bélicos pero cuyas consecuencias no solo pueden afectar a un gobierno y su posicionamiento militar, sino que también la ciudadanía es altamente vulnerable. Se trata de la denominada ciberguerra o guerra cibernética, basada en un conjunto de acciones llevadas a cabo normalmente por un

Estado para penetrar en sistemas informáticos o en las redes de otro país, con la finalidad de causar prejuicio o alteración.

Ante este panorama, medios de comunicación impresos como *ABC, El Mundo* o *El País* prestan escasa atención a fenómenos emergentes a nivel internacional y nacional como son la ciberguerra y los ataques informáticos con fines militares. De los tres diarios objeto de estudio es *El País* el que más espacio le dedica a este tipo de asuntos, seguido de *El Mundo* y relegando a un tercer puesto a *ABC*. De igual forma, el tratamiento suele ser por lo general de tipo informativo, siendo el diario *El Mundo*, junto con *El País*, las cabeceras que más textos opinativos han incluido, lo cual puede reflejar una mayor preocupación por la vigencia y el alcance de las maniobras de ciberataques.

8. BIBLIOGRAFÍA

- ACEROS, J. C. (2006). *Jóvenes, Hacktivismo y Sociedad de la Información* [en línea]. Barcelona: Universidad de Barcelona. http://www20.gencat.cat/docs/Joventut/Documents/Arxiu/OCJ/InformeAceros.pdf (Última consulta: 19/08/2011).
- BUSTAMANTE DONAS, J. (2001). Hacia la cuarta generación de Derechos Humanos: repensando la condición humana en la sociedad tecnológica En: *Revista Iberoamericana de Ciencia, Tecnología e Innovación,* 1. http://www.oei.es/revistactsi/numero1/bustamante.htm (Última consulta: 18/05/2011).
- CÁCERES, S. (2004) Censura y control de contenidos de internet en el mundo. En: *Observatorio de la Sociedad de la Información*, Fundación Orange. http://fundacionorange.es/areas/28_observatorio/obser_01_06.asp (Última consulta: 11/03/2014).
- CLARKE, Richard A. y Knake, Robert K. (2011). *Guerra en la red. Los nuevos campos de batalla*. Barcelona: Ariel.
- CASTELLS, M. (2001) Internet: ¿una arquitectura de libertad? Libre comunicación y control del poder. http://www.uoc.edu/web/esp/launiversidad/inaugural01/internet_arq.htm (Última consulta: 14/02/2014).
- DENNING D. E. (2003). Activismo, Hacktivismo y Ciberterrorismo: Internet como instrumento de influencia en política exterior. En Arquilla, John y Ronfeldt,

David (2001). *Redes y guerras en red. El futuro del terrorismo, el crimen organizado y el activismo político*. Versión castellana de Francisco Muñoz de Bustillo. Madrid: Alianza Editorial.

- DELEUZE, G. (1990). Poruparlers. París: MInuit. (trad. cast.: Conversaciones 1979-1990, Valencia: Pretextos, 1995).
- ECHEVERRÍA, J. (1999): *Los señores del aire: Telépolis y el Tercer Entorno*. Barcelona: Ediciones Destino.
- FACEBOOK (2013). Informe de solicitudes de gobiernos. https://www.facebook.com/about/government_requests (Última consulta: 01/04/2014).
- FACEBOOK (2014). Informe sobre solicitudes gubernamentales. https://govtrequests.facebook.com/ (Última consulta: 01/04/2014).
- GARAIZAR SAGARMINAGA, P. (2004). *El Software Libre como herramienta de hacktivismo contra el cibercontrol social*. Ediciones Simbióticas. http://www.edicionessimbioticas.info/IMG/pdf/ACTIVISMO_Y_SOF_LIBRE.pdf (Última consulta: 14/08/2011).
- FERRERO, Julio Albert (2013). La ciberguerra. Génesis y evolución. En: Revista General de Marina, enero/febrero, Madrid: Editorial MIC, pp. 81-97.
- LYNN, William J. III (2010). Defending a New Domain. En: Foreign Affairs, septiembre/octubre. https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain (Última consulta: 18/05/2014).
- LOBO, J. L. (2013) ¿Nos espía Rajoy? El Gobierno escruta sin control judicial llamadas y correos electrónicos. En: *El Confidencial*, 5 de julio. http://www.elconfidencial.com/espana/2013/07/05/nos-espia-rajoy-el-gobierno-escruta-sin-control-judicial-llamadas-y-correos-electronicos-124355 (Última consulta: 06/07/2013).
- MATTELART, ARMAND y VITALIS, André (2015). *De Orwell al cibercontrol*. Barcelona: Gedisa.
- MELUCCI, A. (1999). *Acción colectiva, vida cotidiana y democracia*. México: El Colegio de México, Centro de Estudios Sociológicos. PMid:10432982.
- PAGET, F. (2012). Hacktivismo. El ciberespacio: nuevo medio de difusión de ideas políticas. McAfee Labs. http://www.mcafee.com/es/resources/white-papers/wp-hacktivism.pdf (Última consulta: 12/02/2014).

- REPORTEROS SIN FRONTERAS (2014). Enemigos de Internet. http://www.rsf-es.org/news/rsf-publica-el-informe-enemigos-de-internet-2014/ (Última consulta: 24/04/2014).
- ROMERO, Pablo (2015). Armados para la 'ciberguerra' fría. En: *Elpais.es*, 15 de febrero. http://www.elmundo.es/espana/2015/02/15/54dfb898e2704e5b7f8b456b.html Última consulta 14/03/2015 (Última consulta: 24/02/2015).
- RT (2013). Google, Microsoft y Apple se benefician de entregar datos al Gobierno de EE.UU. En: *Canal RT*, 11 de julio. http://actualidad.rt.com/actualidad/view/99703-google-microsoft-apple-eeuu-espionaje (Última consulta: 15/07/2013).
- VICENTE, L. (2004). ¿Movimientos sociales en la Red? Los hacktivistas. En: *El Cotidiano*, 20 (126). http://www.redalyc.org/pdf/325/32512615.pdf (Última consulta: 16/11/2013).
- WEGENER, Henning (2013). Los riesgos económicos de la ciberguerra. En *Cuadernos de estrategia*, n. 162, pp. 177-227.
- WIKIPEDIA (2014). Hacktivismo. En: *Wikipedia, la Enciclopedia Libre*. http://es.wikipedia.org/wiki/Hacktivismo (Última consulta: 12/03/2014).

Volver al índice